UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	MISC NO. 10GJ3793 1:11-DM-3

DECLARATION OF STUART A. SEARS IN SUPPORT OF OBJECTIONS OF REAL PARTIES IN INTEREST JACOB APPELBAUM, BIRGITTA JONSDOTTIR, AND ROP GONGRIJP TO MARCH 11, 2011 ORDER DENYING MOTION TO VACATE AND DENYING IN PART MOTION TO UNSEAL

I, STUART A. SEARS, declare and state as follows:

1. I am an attorney licensed to practice law in the Commonwealth of Virginia and am a member of the law firm of Zwerling, Leibig & Moseley, P.C, counsel for the Real Party of Interest Jacob Appelbaum in the above-captioned matter. I have personal knowledge of the facts stated in this Declaration, and if called as a witness I could and would competently testify to them under oath.

2. Attached hereto as Exhibit 1 is a true and correct copy of the December 14, 2010 Court order directing Twitter, Inc. to provide the government with records and other information related to the accounts of several of its users, including the Parties here.

3. Attached hereto as Exhibit 2 is a true and correct copy of excerpts from Birgitta Jonsdottir's Twitter page, http://twitter.com/birgittaj, and Mr. Appelbaum's Twitter page, http://twitter.com/ioerror.

4. Attached hereto as Exhibit 3 is a true and correct copy of the Court Order issued on January 5, 2011.

5. Attached hereto as Exhibit 4 is a true and correct copy of notice from Twitter's Legal Department informing Birgitta Jonsdottir of the record demand dated January 7, 2011.

6. Attached hereto as Exhibit 5 is a true and correct copy of Magistrate Judge Buchanan's March 11, 2011 Memorandum Opinion denying the Motion to Vacate and Motion for Unsealing.

I declare under penalty of perjury that the foregoing is true and correct. Executed this 25th day of March, 2011, at Alexandria, Virginia.

/s/

Stuart A. Sears

EXHIBIT 1

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	MISC. NO. 10GJ3793
	Filed Under Seal

ORDER

This matter having come before the Court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing Twitter, Inc., an electronic communications service provider and/or a remote computing service, located in San Francisco, California, to disclose certain records and other information, as set forth in Attachment A to this Order, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice of this Order to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that Twitter, Inc. will, within three days of the date of this Order, turn over to the United States the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that Twitter shall not disclose the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court.

United States Magistrate Judge

12/14/10
Date

A TRUE COPY
CLERK, U.S. DISTRICT COURT
BY: DEPUTY CLERK

ATTACHMENT A

You are to provide the following information, if available, preferably as data files on CD-ROM, electronic media, or email (tracy.mccormick@usdoj.gov) or otherwise by facsimile to 703-299-3981:

A. The following customer or subscriber account information for each account registered to or associated with Wikileaks; rop_g; ioerror; birgittaj; Julian Assange; Bradley Manning; Rop Gongrijp; Birgitta Jonsdottir for the time period November 1, 2009 to present:

1. subscriber names, user names, screen names, or other identities;
2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
3. connection records, or records of session times and durations;
4. length of service (including start date) and types of service utilized;
5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
6. means and source of payment for such service (including any credit card or bank account number) and billing records.

B. All records and other information relating to the account(s) and time period in Part A, including:

1. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
3. correspondence and notes of records related to the account(s).

EXHIBIT 2

3169. **accessnow** are Nokia Siemens shareholders aware they profit from the sales of monitoring technology? sign the petition: http://bit.ly/bwGrCk #NOtoNOKIA Mon Oct 18 2010 18:37:08 (Pacific Daylight Time) via TweetDeck Retweeted by ioerror and 1 other
3170. Sometimes I really miss working in teledildonics. Mon Oct 18 2010 18:07:24 (Pacific Daylight Time) via web
3171. @auriea I am unsurprised by that answer. That's a bummer for the rest of humanity but likely a relief for her! Mon Oct 18 2010 14:16:32 (Pacific Daylight Time) via web in reply to auriea
3172. @auriea I'm sad about that too. Did you ask Jarboe why she's not touring with them? I'm probably missing something obvious... Mon Oct 18 2010 14:06:40 (Pacific Daylight Time) via web in reply to auriea
3173. **reasonmag** The Horror of Canadian Obscenity Law http://ow.ly/2VnSb Mon Oct 18 2010 12:05:59 (Pacific Daylight Time) via HootSuite Retweeted by ioerror and 13 others
3174. Wow! The Swans are back (without Jarboe) on tour: http://www.metafilter.com/96782/Swans-wasnt-so-bad-after-all Mon Oct 18 2010 11:43:36 (Pacific Daylight Time) via web
3175. @pusscat I agree - though we're gonna need backup! Mon Oct 18 2010 11:34:21 (Pacific Daylight Time) via web in reply to pusscat
3176. Dan Savage rips apart anti-gay marriage arguments so well - it's really impressive. Mon Oct 18 2010 11:33:36 (Pacific Daylight Time) via web
3177. Dan Savage has a special place in my heart: http://www.thestranger.com/seattle/SavageLove?oid=5135029 Mon Oct 18 2010 11:27:28 (Pacific Daylight Time) via web
3178. **torproject** Australia: Internet censorship is now a moral obligation, http://www.theregister.co.uk/2010/10/18/gillard_media/ Mon Oct 18 2010 10:40:27 (Pacific Daylight Time) via identica Retweeted by ioerror and 24 others
3179. @fivetonsflax http://www.expressjetpilots.com/the-pipe/showthread.php?39523-Well-today-was-the-day 9:55 AM Oct 18th, 2010 via web in reply to fivetonsflax
3180. Best quote from the pilot's article on his recent TSA encounter: "Malo Periculosam Libertatem Quam Quietum Servitium" - http://is.gd/g6ZmW 9:50 AM Oct 18th, 2010 via web
3181. **cfpconf** A pilot didn't want to show the TSA his naked body. Here's what happened: http://is.gd/g6OxB #privacy 7:23 AM Oct 18th, 2010 via TweetDeck Retweeted by ioerror and 100+ others
3182. People really dislike the TSA: http://www.elliott.org/blog/travelers-rate-tsa-as-terrible-in-new-poll-they-treat-us-like-we-are-criminals/ 2:19 AM Oct 18th, 2010 via web
3183. Berkman Center accepting fellowship applications for 2011-2012 academic year: http://cyber.law.harvard.edu/node/6413 11:35 PM Oct 17th, 2010 via web
3184. **cathfie** Letter signed by Chinese Communist Party elders blasts government's clampdown on free expression http://bit.ly/aRI03J #Censorship #FOIA 10:16 PM Oct 17th, 2010 via web Retweeted by ioerror and 6 others
3185. **TomDuff** Holy cow, RT @etler: Alcatel-Lucent has put the entire Bell System Technical Journal online for free: http://bstj.bell-labs.com/ 1922-1983. 8:23 PM Oct 17th, 2010 via Twitter for iPad Retweeted by ioerror and 66 others
3186. **pressfreedom** 100+ Chinese scholars, activists, lawyers call for media freedom & release of #LiuXiaobo http://bit.ly/9VTkqp 4:51 PM Oct 15th, 2010 via TweetDeck Retweeted by ioerror and 14 others
3187. Thesis worth reading today: Richard Savacool's Firewall resistance to metaferography in network communications: http://bit.ly/coBJah 9:09 PM Oct 15th, 2010 via web
3188. I really want to meet the guys from gray-world; it's such a great site. The people involved are talented and inspirational. 6:32 PM Oct 15th, 2010 via web
3189. I really do not enjoy being sick. 3:27 PM Oct 15th, 2010 via web
3190. **argvee** Google is looking to hire some thrill-seeking IR and Forensics experts! Tell your friends! http://goo.gl/UNpR 3:20 PM Oct 15th, 2010 via web Retweeted by ioerror and 30 others
3191. **EFF** Sign #NOtoNOKIA petition @accessnow http://bit.ly/ayMOZJ 11:52 AM Oct 14th, 2010 via web Retweeted by ioerror and 14 others
3192. @naskooskov Great - thank you. :-) Perhaps you can join #tor-dev on irc.oftc.net and say you'd like to hack on Tor on Windows? 12:14 PM Oct 14th, 2010 via web in reply to naskooskov
3193. **EFF** Holding Nokia Responsible for Surveilling Dissidents in Iran https://eff.org/r.4tm 11:51 AM Oct

twitter

Login Join Twitter!

http://www.thepetitionsite.com /95/support-the-people-of-iceland

4:49 AM Jan 14th, 2010 via web

birgittaj
Birgitta Jónsdóttir

twitter

Login Join Twitter!

Save the people of Iceland! - http://shar.es/aBovW

5:14 PM Jan 16th, 2010 via web

birgittaj
Birgitta Jónsdóttir

twitter

Login Join Twitter!

http://www.althingi.is/altext/138/s/0688.html http://bit.ly/dtopM3

3:35 PM Feb 19th, 2010 via Facebook

birgittaj
Birgitta Jónsdóttir

twitter

Login Join Twitter!

http://www.immi.is/ http://bit.ly/cpZl6l

2:27 PM Feb 14th, 2010 via Facebook

birgittaj
Birgitta Jónsdóttir

twitter  Login Join Twitter!

Hundreds evacuated after vulcan eroption in Iceland http://bit.ly /9nSImW (via @icerocket)

1:19 AM Mar 21st, 2010 via web

birgittaj
Birgitta Jónsdóttir

twitter

Login Join Twitter!

First video from the volcanic eruption in Iceland - http://bit.ly/iceland_volcanic

1:31 AM Mar 21st, 2010 via bit.ly

birgittaj
Birgitta Jónsdóttir

twitter

Login Join Twitter!

Birgitta Jonsdottir will discuss and introduce the idea behind immi.is at eurodig.org tomorrow http://bit.ly /asTung - live webcast...

2:26 AM Apr 28th, 2010 via web

birgittaj
Birgitta Jónsdóttir

EXHIBIT 3

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE §2703(d) ORDER RELATING TO TWITTER ACCOUNTS: WIKILEAKS, ROP_G; IOERROR; AND BIRGITTAJ	)))))	MISC. NO. 10GJ3793

ORDER TO UNSEAL THE
ORDER PURSUANT TO 18 U.S.C. §2703(D)

This matter having come before the Court pursuant to an application under Title 18, United States Code, §2703(d), it appearing that it is in the best interest of the investigation to unseal the Court's Order of December 14, 2010 and authorize Twitter to disclose that Order to its subscribers and customers, it is hereby ORDERED that the above-captioned Order of December 14, 2010 pursuant to 18 U.S.C. §2703(d) be UNSEALED and that Twitter is authorized to disclose such Order. In all other respects, the Court's Order of December 14, 2010 remains in effect.

THE HONORABLE THERESA C. BUCHANAN
UNITED STATES MAGISTRATE JUDGE

Date: 1/5/11

Alexandria, Virginia

EXHIBIT 4

Subject: Fwd: #1466264 Twitter Support: update on "Twitter Receipt of Legal Process"

From: Birgitta Jonsdottir [redacted]
Sent: Friday, January 07, 2011 7:10 PM
Subject: Fwd: #1466264 Twitter Support: update on "Twitter Receipt of Legal Process"

Begin forwarded message:

From: Kessel [redacted]
Date: January 7, 2011 7:21:05 PM GMT
To: birgittaj [redacted]
Subject: #1466264 Twitter Support: update on "Twitter Receipt of Legal Process"
Reply-To: Twitter Support <support+id1466264@twitter.zendesk.com>

Please do not write below this line -##

Kessel, Jan-07 11:20 am (PST):

Dear Twitter User:

We are writing to inform you that Twitter has received legal process requesting information regarding your Twitter account, @birgittaj. A copy of the legal process is attached. The legal process requires Twitter to produce documents related to your account.

Please be advised that Twitter will respond to this request in 10 days from the date of this notice unless we receive notice from you that a motion to quash the legal process has been filed or that this matter has been otherwise resolved.

To respond to this notice, please e-mail us at twitter-legal@twitter.com.

This notice is not legal advice. You may wish to consult legal counsel about this matter. If you need assistar seeking counsel, you may consider contacting the Electronic Frontier Foundation (Kevin Bankston: bankston@eff.org, +1 415 436 9333 x126) or the ACLU (Aden Fine: afine@aclu.org, (212) 549-2693).

Sincerely,

Twitter Legal

Attachment(s)
20101214160501127.pdf
Twitter_Unsealing Order.pdf

EXHIBIT 5

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

In Re: §2703(d) Order; 10GJ3793	)	Miscellaneous No. 1:11dm00003

MEMORANDUM OPINION

This matter came before the Court the Motion of Real Parties in Interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp to Vacate December 14, 2010 Order ("Motion to Vacate", Dkt. 1) and Motion of Real Parties in Interest Jacob AppelBaum, Rop Gonggrijp, and Birgitta Jonsdottir for Unsealing of Sealed Court Records. ("Motion to Unseal", Dkt. 3). For the following reasons, petitioners' Motion to Vacate is DENIED, and petitioners' Motion to Unseal is DENIED in part, GRANTED in part, and taken under further consideration in part.

BACKGROUND

Petitioners are Twitter users associated with account names of interest to the government. Petitioner Jacob Appelbaum (Twitter name "ioerror") is a United States citizen and resident, described as a computer security researcher. (Pet. Motion to Unseal at 3). Rop Gonggrijp (Twitter name "rop_g") is a Dutch citizen and computer security specialist. *Id*. Birgitta

Jonsdottir (Twitter name "birgittaj") is an Icelandic citizen and resident. She currently serves as a member of the Parliament of Iceland. *Id*.

On December 14, 2010, upon the government's *ex parte* motion, the Court entered a sealed Order ("Twitter Order") pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act, which governs government access to customer records stored by a service provider. 18 U.S.C. §§ 2701-2711 (2000 & Supp. 2009). The Twitter Order, which was unsealed on January 5, 2010, required Twitter, Inc., a social network service provider, to turn over to the United States subscriber information concerning the following accounts and individuals: Wikileaks, rop_g, ioerror, birgittaj, Julian Assange, Bradely Manning, Rop Gonggrijp, and Birgitta Jonsdottir. In particular, the Twitter Order demands:

A. The following customer or subscriber account information for each account registered to or associated with Wikileaks; rop_g; ioerror; birgittaj; Julian Assange; Bradely Manning; Rop Gongrijp [*sic*.]; Birgitta Jonsdottir for the time period November 1, 2009 to present:
    1. subscriber names, user names, screen names, or other identities;
    2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
    3. connection records, or records of session times and durations;
    4. length of service (including start date) and types of service utilized;
    5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
    6. means and source of payment for such service (including any credit card or bank account number) and billing records.

B. All records and other information relating to the account(s) and time period in Part A, including:
   1. records of user activity for any connections made to or from the Account, including date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
   2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
   3. correspondence and notes of records related to the account(s).

On January 26, 2011, petitioners filed the instant motions asking the Court to vacate the Twitter Order, and to unseal all orders and supporting documents relating to Twitter and any other service provider. Moreover, petitioners request a public docket for each related order. On February 15, 2011, the Court held a public hearing and took petitioners' motions under consideration. For the following reasons, the Court declines to vacate the Twitter Order, and orders that only documents specified below shall be unsealed.

ANALYSIS

I. Motion to Vacate

Petitioners request that the Twitter Order be vacated. The parties have raised the following issues in their briefs: (1) whether petitioners have standing under the Stored Communications Act ("SCA") to bring a motion to vacate, (2) whether the Twitter Order was properly issued under 18 U.S.C. §2703, (3) whether the Twitter Order violates petitioners' First Amendment rights, (3)

whether the Twitter Order violates petitioners' Fourth Amendment rights, and (4) whether the Twitter Order should be vacated as to Ms. Jonsdottir for reasons of international comity.

(1) Petitioners' Standing Under 18 U.S.C. §2704(b)

Pursuant to §2704(b)(1)(A), a customer may challenge a §2703(d) order only upon an affidavit "stating that the applicant is a customer or subscriber to the service from which the ***contents*** of electronic communications maintained for him have been sought." (emphasis supplied). The Court holds that targets of court orders for non-content or records information may not bring a challenge under 18 U.S.C. §2704, and therefore, petitioners lack standing to bring a motion to vacate the Twitter Order.

The SCA provides greater protection to the "contents of electronic communications", sought pursuant to §2703(a) and §2703(b), than to their "records" (§2703(c)). The statutory definition of "contents" is "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. §2711(1); 18 U.S.C. §2510(8)(2002). Targets of content disclosures are authorized to bring a customer challenge under §2704. Conversely, §2703(c)(1) describes "records" as "a record or other information pertaining to a subscriber to or customer of such service (not the contents of communication)." According to §2703(c)(2), records include:

> (A) name;
> (B) address;
> (C) local and long distance telephone connection records, or records of session times and durations;

> (D) length of service (including start date) and types of service utilized;
> (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
> (F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses...*any means available under paragraph* (1) (emphasis supplied).

The Twitter Order does not demand the contents of any communication, and thus constitutes only a request for records under §2703(c). Even though the Twitter Order seeks information additional to the specific records listed in §2703(c)-- data transfer volume, source and destination Internet Protocol addresses, and [Twitter's] correspondence and notes of records related to the accounts -- these, too, are non-content "records" under §2703(c)(1). Therefore, as the targets of mere records disclosure, petitioners may not bring a customer challenge under §2704.

Petitioners, unable to overcome the language of §2704, assert in reply that they have standing based on general due process, but cite no authority on point. Moreover, §2704 seems to recognize that only targets of content disclosures would have a viable constitutional challenge to the compelled disclosure of private communications. Customers who voluntarily provide non-content records to an internet service provider would not enjoy the same level of protection.

(2) Proper Issuance of the Twitter Order

Notwithstanding petitioners' lack of standing to bring their motion to vacate, the Court finds that the substance of their motion is equally unavailing.

The Twitter Order came before the Court upon the government's motion and supporting application for an order pursuant to 18 U.S.C. §2703(d). Section 2703(d) provides in pertinent part:

> "(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are *relevant and material* to an ongoing criminal investigation." (emphasis supplied).

On December 14, 2010, the Court found that the application satisfied §2703(d) and entered the Twitter Order. Petitioners now ask the Court to reconsider the sufficiency of the underlying application pursuant to §2704(b)(1)(B), which authorizes customers to move to vacate an order upon a showing "that there has not been substantial compliance" with §2703(d). Because the application remains sealed, petitioners face the difficulty of challenging a document they have not seen. Nevertheless, petitioners speculate that regardless of the application's factual support, it could not have justified the scope of the Twitter Order. That is, petitioners contend that because their publically posted "tweets" pertained mostly to non-Wikileaks topics, the Twitter Order necessarily demands data that has no connection to Wikileaks and cannot be "relevant or material" to any ongoing investigation as §2703(d) requires. Notwithstanding

petitioners' questions, the Court remains convinced that the application stated "specific and articulable" facts sufficient to issue the Twitter Order under §2703(d). The disclosures sought are "relevant and material" to a legitimate law enforcement inquiry. Also, the scope of the Twitter Order is appropriate even if it compels disclosure of some unhelpful information. Indeed, §2703(d) is routinely used to compel disclosure of records, only some of which are later determined to be essential to the government's case. Thus, the Twitter Order was properly issued pursuant to §2703(d).

As an alternative, petitioners propose that, even if the government has stated facts sufficient to meet the §2703(d) "relevant and material" standard, the Court should use its discretion to require the government to meet the probable cause standard required for a search warrant. *See In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 315-17 (3d Cir. 2010). The Court declines to deviate from the standard expressly provided in §2703(d). At an early stage, the requirement of a higher probable cause standard for non-content information voluntarily released to a third party would needlessly hamper an investigation. *See In re Subpoena Duces Tecum*, 228 F.3d 341, 348-39 (4th Cir. 2000). Therefore, the Court finds that the Twitter Order was properly issued.

(3) First Amendment Claim

Petitioners claim the Twitter Order allows the government to create a "map of association" that will have a chilling effect on their First Amendment rights.[1]

The First Amendment guarantees freedom of speech and assembly.[2] Recognizing the "close nexus between freedoms of speech and assembly", the Supreme Court has established an implicit First Amendment right to freely associate. *N.A.A.C.P. v. Alabama ex rel. Patterson*, 357 U.S. 449,460 (1958). The freedom of association may be hampered by compelled disclosure of a political or religious organization's membership. *Id*. at 462 (preventing compelled disclosure of NAACP membership list). However, the freedom of association does not shield members from cooperating with legitimate government investigations. *United States v. Mayer,* 503 F.3d 740, 748 (9th Cir. 2007). Other First Amendment interests also yield to the investigatory process. *Brazenburg v. Hayes*, 408 U.S. 665, 682, 691 (1972)(freedom of the

---

[1]Though they assert First and Fourth Amendment claims, petitioners cite no authority as to the applicability of the United States Constitution to non-citizens residing and acting outside of the U.S. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990)(Fourth Amendment inapplicable where American authorities searched the home of a Mexican citizen and resident, who had no voluntary attachment to the United States; *Wang v. Reno*, 81 F.3d 808,817-18 (9th Cir. 1996)(alien entitled to 5th Amendment due process rights only after government created "special relationship with alien" by paroling him from China to U.S. to testify at drug trial). The Court has serious doubts as to whether Ms. Jonsdottir and Mr. Gonggrijp enjoy rights under the U.S. Constitution.

[2]"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.

press); *University of Pennsylvania v. E.E.O.C.*, 493 U.S. 182, 197-98 (1990)(academic freedom). In the context of a criminal investigation, a district court must "balance the possible constitutional infringement and the government's need for documents...on a case-by-case basis and without putting any special burden on the government", and must also prevent abuse. *In re Grand Jury 87-3 Subpoena Duces Tecum*, 955 F.2d 229,234 (4th Cir. 1992).[3] Accordingly, a subpoena should be quashed where the underlying investigation was instituted or conducted in bad faith, maliciously, or with intent to harass. *Id.*[4]

The Court finds no cognizable First Amendment violation here. Petitioners, who have already made their Twitter posts and associations publicly available, fail to explain how the Twitter Order has a chilling effect. The Twitter Order does not seek to control or direct the content of petitioners' speech or association. Rather, it is a routine compelled disclosure of non-content information which petitioners voluntarily provided to Twitter pursuant to Twitter's Privacy Policy. Additionally, the

---

[3]Other circuits have adopted a "substantial relationship" test, whereby the government must show its subpoena serves a compelling interest that outweighs any alleged chilling effect. But even courts that have adopted the test regularly refuse to quash subpoenas on First Amendment grounds. *See In re Grand Jury Proceedings,* 776 F.2d 1099,1103 (2d Cir. 1985)(requiring cooperation with pre-indictment proceedings); *In re Grand Jury Subpoenas Duces Tecum*, 78 F.3d 1307, 1312-13(8th Cir. 1996)(same); *In re Grand Jury Proceedings*, 842 F.2d 1229,1236-37 (11th Cir. 1988)(same).

[4]Most cases dealing with First Amendment challenges in the pre-indictment phase involve subpoenas, not §2703(d) court orders. However, §2703(d) orders resemble subpoenas because they also compel disclosure of documents.

Court's §2703(d) analysis assured that the Twitter Order is reasonable in scope, and the government has a legitimate interest in the disclosures sought. *See In re Grand Jury 87-3 Subpoena Duces Tecum*, 955 F.2d at 234. Furthermore, there is no indication of bad faith by the government. *Id.* Thus, petitioners' First Amendment challenge to the Twitter Order fails.

(4) Fourth Amendment Claim

Petitioners argue that the Twitter Order should be vacated because it amounts to a warrantless search in violation of the Fourth Amendment. In particular, petitioners challenge the instruction that Twitter, Inc. produce the internet protocol addresses ("IP addresses") for petitioners' Twitter accounts for specified dates and times. Petitioners assert a Fourth Amendment privacy interest in their IP address information, which they insist are "intensely revealing" as to location, including the interior of a home and movements within.

The Fourth Amendment provides that "the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable cause..." U.S. CONST. amend. IV. Not all investigatory techniques by the government implicate the Fourth Amendment. A government action constitutes a "search" only if it infringes on an expectation of privacy that society considers reasonable. *United States v. Jacobsen*, 466 U.S. 109,113 (1984). Thus, the government must obtain a warrant before inspecting places where the public

traditionally expects privacy, like the inside of a home or the contents of a letter. *United States v. Karo,* 468 U.S. 705, 714 (1984)(warrant required to use electronic location-monitoring device in a private home); *Kyllo v. United States*, 533 U.S. 27, 34 (2001)(warrant required to use publically unavailable, sense-enhancing technology to gather information about the interior of a home); *Jacobsen*, 466 U.S. at 114 (warrant required to inspect the contents of sealed letters and packages); *See also United States v. Warshak*, 2010 WL 5071766 at 13-14 (6th Cir. 2010)(extending Fourth Amendment protection to the contents of certain email communications).

On the other hand, the Fourth Amendment privacy expectation does not extend to information voluntarily conveyed to third parties. For example, a warrantless search of bank customers' deposit information does not violate the Fourth Amendment, because there can be no reasonable expectation of privacy in information voluntarily conveyed to bank employees. *United States v. Miller*, 425 U.S. 435, 442 (1976). Similarly, the Fourth Amendment permits the government to warrantlessly install a pen register to record numbers dialed from a telephone because a person voluntarily conveys the numbers without a legitimate expectation of privacy. *Smith v. Maryland*, 442 U.S. 735 (1979).

With these principles in mind, the Fourth Circuit has held that no legitimate expectation of privacy exists in subscriber information voluntarily conveyed to phone and internet companies. *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010)(citing *Smith v. Maryland*, 442 U.S. at 744). In *Bynum*, the defendant,

who was convicted of child pornography charges, challenged the constitutionality of administrative subpoenas the government used to collect information from his internet and phone companies, including his name, email address, phone number, and physical address. *Id.* Holding that the subpoenas did not violate the Fourth Amendment, the *Bynum* Court reasoned that the defendant had no expectation of privacy in information he voluntarily conveyed, and that in doing so, he assumed the risk that the companies would turn it over to authorities. *Id.* Moreover, "every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment." *Id.* at 164. Accordingly, several circuits have declined to recognize a Fourth Amendment privacy interest in IP addresses.[5] *United States v. Christie*, 624 F.3d 558,574 (3d Cir. 2010)("no reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs"); *United States v. Forrester*, 512 F.3d 500,510 (9th Cir. 2008); *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008); *see also Bynum*

[5] Petitioners highlight the Supreme Court's admonition that courts should avoid unnecessary rulings on how the Fourth Amendment applies to new technologies. *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629, 177 L. Ed. 2d 216 (2010). There, in a case involving employer-provided electronic communication devices, the Court said "the judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear". Here several courts have encountered IP address issues. This is not "emerging technology" worthy of constitutional avoidance.

604 F.3d at 164 n.2 (stating that defendant's IP address amounts to numbers that he "never possessed").

Here, petitioners have no Fourth Amendment privacy interest in their IP addresses. The Court rejects petitioners' characterization that IP addresses and location information, paired with inferences, are "intensely revealing" about the interior of their homes. The Court is aware of no authority finding that an IP address shows location with precision, let alone provides insight into a home's interior or a user's movements. Thus the *Kyllo* and *Karo* doctrines are inapposite. Rather, like a phone number, an IP address is a unique identifier, assigned through a service provider. *Christie*, 624 F.3d at 563; *Smith v. Maryland*, 442 U.S. at 744. Each IP address corresponds to an internet user's individual computer. *Christie*, 624 F.3d at 563. When a user visits a website, the site administrator can view the IP address. *Id.* Similarly, petitioners in this case voluntarily conveyed their IP addresses to the Twitter website, thus exposing the information to a third party administrator, and thereby relinquishing any reasonable expectation of privacy.

In an attempt to distinguish the reasoning of *Smith v. Maryland* and *Bynum,* petitioners contend that Twitter users do not directly, visibly, or knowingly convey their IP addresses to the website, and thus maintain a legitimate privacy interest. This is inaccurate. Before creating a Twitter account, readers are notified that IP addresses are among the kinds of "Log Data" that Twitter collects, transfers, and manipulates. *See Warshak*, 2010

WL 5071766 at *13 (recognizing that internet service provider's notice of intent to monitor subscribers' emails diminishes expectation of privacy). Thus, because petitioners voluntarily conveyed their IP addresses to Twitter as a condition of use, they have no legitimate Fourth Amendment privacy interest. *Smith*, 422 U.S. at 744; *Bynum*, 604 F.3d at 164.[6]

(5) International Comity

Petitioners argue the Twitter Order should be vacated as to Ms. Jonsdottir, a member of the Icelandic Parliament.[7] Petitioners warn of a threat to international comity, which is defined as "the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws." *In re French v. Liebmann*, 440 F.3d 145,152 (4th Cir. 2006)(*citing Hilton v. Guyot*, 159 U.S. 113, 164 (1895).

---

[6]At the hearing, petitioners suggested that they did not read or understand Twitter's Privacy Policy, such that any conveyance of IP addresses to Twitter was involuntary. This is unpersuasive. Internet users are bound by the terms of click-though agreements made online. *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 544 F.Supp.2d 473,480 (E.D. Va. 2008)(finding a valid "clickwrap" contract where users clicked "I Agree" to acknowledge their acceptance of the terms)(*aff'd A.V. ex rel v. iParadigms, LLC*, 562 F.3d 630,645 n.8 (4th Cir. 2009). By clicking on "create my account", petitioners consented to Twitter's terms of use in a binding "clickwrap" agreement to turn over to Twitter their IP addresses and more.

[7]The Court thanks the Inter-Parliamentary Union for its *Amicus* Brief on this issue.

The threshold question in international comity analysis is whether there is a conflict between foreign and domestic law. *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court.*, 482 U.S. 522, 555 (1987). A corollary of international comity is the established presumption against extraterritorial application of American statutes. *In re French,* 440 F.3d at 149, 151.

Here, petitioners have not asserted any conflict between American and Icelandic Law implicating international comity concerns. Instead, petitioners assert that the disclosures sought could not be obtained under Icelandic law, which affords strong immunity to members of parliament. According to the Inter-Parliamentary Union, Icelandic parliamentary immunity "ensures that members of parliament cannot be held to account for the opinions they express and the votes they cast..." (Sears Decl. Ex. 6). Here, the Twitter Order does not violate this provision. It does not ask Ms. Jonsdottir to account for her opinions. It does not seek information on parliamentary affairs in Iceland, or any of Ms. Jonsdottir's parliamentary acts. Her status as a member of parliament is merely incidental to this investigation. Also, neither petitioners nor the Inter-Parliamentary Union have cited authority to support their assumption that Icelandic immunity extends to public "tweets". In the United States, such public statements are not regarded as part of the legislative function or process, and thus would not invoke the legislative immunity of the Constitution's Speech and Debate Clause. *Hutchinson v. Proxmire*, 443 U.S. 111, 132 (1979)(no legislative immunity for statements "scattered far and

wide by mail, press, and the electronic media"); *United States v. Gravel*, 408 U.S. 606, 616 (1972). Nor would a member of Congress be permitted to invoke her position to avoid being a witness in a criminal case. *Gravel*, 408 U.S. at 622. Thus, the Court rejects the assertion that the Twitter Order is a clash of American and Icelandic law that threatens international comity.

Moreover, in accordance with international comity, the Twitter Order is not an extraterritorial application of American law. Rather, it is a routine request for information pursuant to a valid act of the United States Congress, the Stored Communications Act. It compels disclosures from Twitter, an American corporation, and requires nothing of Ms. Jonsdottir. When Ms. Jonsdottir consented to Twitter's Privacy Policy she assumed the risk that the United State's government could request such information. For these reasons, the Court declines to vacate the Twitter Order as to Ms. Jonsdottir.

II. Motion to Unseal

The documents in this matter, 1:11-dm-00003, were initially sealed by the Clerk's office. Petitioners now ask that all documents within this file be unsealed. According to the parties' agreement, sealing is no longer necessary for the 1:11-dm-00003 docket, with the exception of Government's Response in Opposition to the Real Parties' in Interest Motion for Unsealing of Sealed Court Records (Dkt. 22) and Twitter's Motion for Clarification (Dkt. 24), to which the government still objects.

Petitioners further request the unsealing of the application in support of the Twitter Order and all other documents in case

number 10-gj-3793. Additionally, to the extent any other companies received similar orders, petitioners request the unsealing of those orders and their applications. Petitioners also request a public docket of such material.

Petitioners have no right of access to the sealed documents supporting the Twitter Order in case number 10-gj-3793. At the pre-indictment phase, "law enforcement agencies must be able to investigate crime without the details of the investigation being released to the public in a manner that compromises the investigation." *Va. Dept. of State Police v. Washington Post*, 386 F.3d 567, 574 (4th Cir. 2004). Secrecy protects the safety of law enforcement officers and prevents destruction of evidence. *Media General Operations v. Buchanan*, 417 F.3d 424,429 (4th Cir. 2005). It also protects witnesses from intimidation or retaliation. *In re Grand Jury Investigation of Cuisinarts, Inc.*, 665 F.2d 24, 27-28 (2d Cir. 1981). Additionally, secrecy prevents unnecessary exposure of those who may be the subject of an investigation, but are later exonerated. *Douglas Oil Co. V. Petrol Stops N.W.*, 441 U.S. 211, 219 (1979). For these reasons, sensitive investigatory material is appropriately sealed. *Va. Dept. of State Police*, 386 F.3d at 589.

In spite of these considerations, petitioners claim this material should be accessible pursuant to the common law presumption that public documents, including judicial records, are open and available for citizens to inspect. *Media General Operations v. Buchanan*, 417 F.3d 424, 429 (4th Cir. 2005)(citing *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 597-98

(1978). The common law presumption of openness may be overcome by a countervailing government interest. *Id.*; *Rushford v. New Yorker Magazine*, 846 F.2d 249, 253 (4th Cir. 1988). Petitioners contend that the government's interest in continued sealing does not outweigh the public's interest in debating internet privacy issues and Wikileaks. Also, petitioners insist that the publicity surrounding the Twitter Order has rendered moot the traditional reasons for secrecy. This is unconvincing. *See United States v. Moussaoui*, 65 F. App'x 881, 887 n.5 (4th Cir. 2003)(rejecting argument that publicity justifies unsealing in high profile terrorism case). Petitioners' argument ignores the significant difference between revealing the existence of an investigation, and exposing critical aspects of its nature and scope. The sealed documents at issue set forth sensitive nonpublic facts, including the identity of targets and witnesses in an ongoing criminal investigation. Indeed, petitioners present no authority for the proposition that the public has a right of access to documents related to an ongoing investigation. *Cf. In the Matter of Application and Affidavit for a Search Warrant*, 923 F.2d 324,326 (4th Cir. 1991)(affirming decision to unseal affidavit only after investigation had concluded). Because the government's interest in keeping these documents sealed for the time being outweighs petitioners' interest in accessing them, there is no common law right of access to the requested judicial records.

Petitioners also assert a First Amendment right of public access to the sealed documents. The First Amendment provides a

right of access only when (1) the place or process to which access is sought has been historically open to the public, and (2) public access plays a significant positive role in the particular process. *Baltimore Sun v. Goetz*, 886 F.2d 60, 63-64 (4th Cir. 1989). As set forth above, there is no history of openness for documents related to an ongoing criminal investigation. Additionally, there are legitimate concerns that publication of the documents at this juncture will hamper the investigatory process. Thus, there is no First Amendment justification for unsealing the 10-gj-3793 documents.

Concerning petitioners' request for public docketing of 10-gj-3793, this requires further review and will be taken under consideration.

Regarding case number 1:11-dm-00003, the Court has reviewed the redactions requested by the government as to docket numbers 22 and 24. As to the Government's Response in Opposition to the Real Parties' in Interest Motion for Unsealing of Sealed Court Records (Dkt. 22), the Court finds that the proposed redactions do not reveal any sensitive investigatory facts which are not already revealed by the Twitter Order. Therefore, it shall be unsealed. The government's remaining proposed redaction is the email address of a government attorney appearing on Twitter, Inc.'s Motion for Clarification. (Dkt. 24). The Court finds that this redaction is appropriate, and the redacted version of Twitter Inc.'s motion shall be released.

CONCLUSION

For the foregoing reasons, petitioners' Motion to Vacate is DENIED. Petitioners' Motion to Unseal is DENIED as to docket 10-gj-3793, and GRANTED as to the 1:11-dm-00003 docket, with the exception of the government attorney's email address in Twitter's Motion for Clarification (Dkt. 24), which shall be redacted. Petitioners' request for public docketing of the material within 10-gj-3793 shall be taken under consideration. An Order shall follow.

/s/
THERESA CARROLL BUCHANAN
UNITED STATES MAGISTRATE JUDGE

March 11, 2011
Alexandria, Virginia